Poole Grammar School	Policy	PGS/P/31
Data Protection Policy and the General Data Protection Regulation May 2018		Issue 3
		May 2018

GENERAL STATEMENT

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the current Data Protection Act 1998 which will be superseded by the General Data Protection Regulation (GDPR) that come into force on 25 May 2018. Compliance with the Freedom of Information Act is contained in a separate policy.

Under the GDPR, everyone is responsible for good data management and processing. All staff involved with the collection, processing and disclosure of personal data are data processors and need to be aware of their duties and responsibilities within these guidelines.

ROLES

The GDPR defines the following roles:

Role	Performed by
Data Protection Controller	Poole Grammar School Governing Body
Data Protection Officer	A trained IT-skilled Governor (Data Responsible Officer)
Data Protection Advisor(s)	Data Manager, Deputy Head (Data)
Data Processor	All school employees processing or managing data

ENQUIRIES

Information about the school's GDPR Policy is available through the Bursar/Clerk to the Governors. General information about the GDPR can be obtained from the Information Commissioner's Office (ICO) 0303 123 1113 option 4 (small organisation advice) or www.ico.org.uk

DEFINITIONS

Data is any information relating to an identified or identifiable natural person (**data subject**).

An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Data – the following categories of data are considered sensitive – racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic data, and biometric data.

6 GDPR PRINCIPLES

From May 2018, six data protection principles will require that personal data should be:

a. Processed in a fair, lawful and transparent manner;
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. Adequate, relevant and limited to what is necessary;
d. Accurate and where necessary kept up to date (inaccurate data should be erased or rectified without delay);
e. Kept in a form permitting identification for no longer than is necessary;
f. Processed in a manner ensuring appropriate security of personal data.

FAIR OBTAINING AND PROCESSING

Poole Grammar School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is included on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

REGISTERED PURPOSES – INFORMATION COMMISSIONER'S OFFICE

The Data Protection Registration entries for the School are available for inspection by appointment at the Bursar's office. The Certificate of Registration for Poole Grammar School is held by the Bursar's office.

DATA INTEGRITY

The School undertakes to ensure data integrity by the following methods:

Data Accuracy – Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. A form ('Updating Student Information') is available on the School website to facilitate this. Primary contacts of students will be prompted annually to check details either electronically via the Parent app or, if non-subscribers to this, via a printout of the student's data record.

Where a data subject challenges the accuracy of their data, the School will mark the record as "challenged". In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the "challenged" marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance - Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The Headteacher, Deputy Headteacher (Data) and the Data Manager will meet annually, usually in the summer term, to review the relevancy of records.

Length of Time – Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Deputy Headteacher (Data) to ensure that obsolete data are properly erased.

SUBJECT ACCESS REQUEST (SAR)

The Data Protection Act and General Data Protection Regulation extend to all data subjects a right of access to their own personal data and other supplementary information (as detailed in the school's privacy notices) to allow individuals to be aware of and verify the lawfulness of the processing by the school. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Charges for or Refusal of a Subject Access Request

Under normal circumstances, a copy of the information requested will be provided free of charge. However, a reasonable fee (taking into account the administrative costs of providing the information) can be charged or, in extreme circumstances, subject access requests can be refused, on the grounds that they are:

- Manifestly unfounded, or
- Excessive, in particular because they are repetitive.

Where the school refuse to respond to a request, it will explain why to the individual, informing them of their right to complain to the Deputy Headteacher (Data) and to judicial remedy without undue delay and at the latest within one month.

When estimating the cost of SAR compliance, the cost of each of the following administrative activities is taken into account:

- Determining whether the school holds the information;
- Finding the requested information, or records containing the information;
- Retrieving the information or records;
- Extracting and processing the requested information from records.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a 'Subject Access Request' form, available from the School Office. Completed forms should then be submitted to the Deputy Headteacher (Data). Provided there is sufficient information to process the request, an entry will be made in the Subject Access Log Book, showing the date of receipt, the data subject's name, the name and address of the requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information - normally 40 calendar days from the request date. This can be extended if the request(s) are amended or added to and the school will inform the individual why an extension is necessary and the likely additional school days required to meet the request(s). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Note: As the school is an academy and not a maintained school, the Education (Pupil Information) (England) Regulations are used by the school as guidelines as they are not legally binding to non-maintained schools. However, in the case of any written request from a parent regarding their own child's educational record citing the Education (Pupil Information) Regulations, this will be treated as a Subject Access Request and will additionally require the permission of the student for release of their information in line with any current data protection regulations. The only exceptions that would be made to acceding to a request for a child's records are if the information supplied:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would mean releasing examination marks before they are officially announced

Similarly, only students may correspond with the school exams office regarding results unless a nominated person has been pre-arranged and, under no circumstances will results information be discussed over the phone. It should be noted that students' personal data will be shared with exam boards as required for the processing and recording of results.

AUTHORISED DISCLOSURES

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's Data Protection Advisor/other authorised school staff may need to disclose data without explicit consent for that occasion eg safeguarding considerations. If this is necessary, they will consult with the Headteacher before doing so.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare (see Privacy Statements).
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

  A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

  An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

DATA AND COMPUTER SECURITY

Poole Grammar School undertakes to ensure security of personal data by following general methods:

Physical Security - Appropriate building security measures are in place which include internal and external CCTV, alarms, door and window locks, secure cabinets and stores. Laptops, IT tablets, memory sticks, disks, tapes and printouts are to be locked away securely when not in use. Visitors to the school are required to

sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied. Staff and Governors are required to wear identification badges while on the school premises.
Logical Security - Security software is installed on the network and other authorised school machines. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies taken) regularly.

IT Security – In addition to the physical security measures, employees are advised to password protect sensitive files, encrypt where appropriate, and take particular care when circulating sensitive personal data. Memory sticks must be protected and kept secure. Encryption is required for all IT/communication devices that may be used off the school premises that access or use personal data.

Procedural Security - In order to be given authorised access to the network, staff will have to undergo DBS and list 99 checks as part of a contract to acknowledge confidentiality. All staff are trained in their data protection obligations and their knowledge updated as necessary. Refresher training is to be on an onward basis. Sensitive computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Governing Body as Data Protection Controller. It is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the Deputy Headteacher (Data) and Data Manager.

THIRD PARTIES AND COMPLIANCE

The GDPR requires organisations to check the compliance of their main suppliers. The Department for Education have a listing of approved suppliers on their website who satisfy the GDPR.

Data and the Cloud – Data cannot be sent outside of the safety of the EU/Norway/Switzerland except in specified circumstances. The IT Manager must ensure any third party supplier that use cloud servers for storing school data that these servers are located in the EU.

BREACHES, REPORTING AND SANCTIONS

Breach - A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Reporting - Breaches must be reported as soon as possible to the Deputy Head (Data) or in their absence the Bursar or Data Manager who will assess the severity of the breach to people's rights and freedoms. If there is a risk, then the ICO and the School's Data Protection Officer need to be informed.

The ICO needs to be informed within 72 hours of a beach being discovered. Details include how the breach happened, what information has gone missing, the potential consequences, what is being done to retrieve it and/or mitigate it, measure being taken and future plans to prevent a similar future event.

Sanctions - Individual members of staff can be personally liable in law under the terms of the GDPR. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data.

A breach of the GDPR may be treated as a disciplinary matter if the school policies are not adhered to, and serious breaches could lead to dismissal.

MONITORING COMPLIANCE AND AUDITS

The Data Protection Officer (DPO) has the responsibility of working with the Data Protection Advisors to monitor compliance with the GDPR and other legal data protection requirements including the school's policies relating to this. The DPO will audit the school on an annual basis and will inform and advise the Data Protection Controllers (Full Governors) and Data Protection Advisors on any compliance issues.

In the event of a breach, this would be served on the Data Protection Controllers, and the DPO would act as the contact point for the supervisory authority (ICO)

CONSENT PROCEDURE

In line with the GDPR, the school has a consent procedure covering students and employees. This outlines how the school seeks, records and manages consent. It also covers how parents/guardians can withdraw consent for information gathered through the Student Information Form.

ParentPay has been adapted to record parental consent for school trips and activities. The Finance Office manage a consent procedure for student access to biometric or pincode devices used for the school's cashless catering system.

COMPLAINTS POLICY

The complaints policy and form is posted on the school website.

LINKED POLICIES AND PROCEDURES

The following are available on the school website and in the school policies section of Moodle. It is mandatory that all staff familiarise themselves with these:

Available via School Website – The School – Policies:

- Consent Procedure
- Privacy Statement – School Workforce
- Privacy Statement – Students

Available via Moodle – Staff Room – School Policies – Documents – Academy Policies:

- CCTV Policy
- Information Security Policy
- Internet Email Usage Security Policy
- Password Security Policy
- Records Management Policy
- Retention Schedule – Appendix 1 to Records Management Policy
- Taking Using Storing Pupil Images Policy

Authors	Donna London, Dee Cheminant, Jonathan Stiby	
Reviewed by	SLT, Premises Governors	April 2018
Approved by	Full PGS Governors	April 2018
Next Review if required		At an appropriate date after GDPR introduction